CLAIMS

Claim 1: A method and apparatus to secure online transactions over the phone comprising:

- a smart card transmitting a identification sequence to an IVR server in the form of a modulated signal,
- a card reader plugged into the telephone line,
- an IVR applet demodulating the identification sequence,

and characterized by the absence of processing means within the card reader.

Claim 2: A method as in claim 1, wherein the identification sequence comprises at least a unique card number and a random number valid only once.

Claim 3: A method as in claim 2, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

Claim 4: A method as in claim 3, wherein the session key (Ki) is a function of the previous one (Ki-1) emitted by the card such as: Ki = G(Ki-1), G is a one-way function also known by the authentication server.

Claim 5: A method as in claim 4, wherein the session key (Ki) is used by the IVR applet to encrypt the PIN entered by the user; said encryption code is transmitted to the authentication server along with the card number.

Claim 6: A method as in claim 5, wherein the authentication server decrypts the encryption code to retrieve the user PIN, using a session key deduced from the previous one (Ki-1) stored in the authentication server database.

Claim 7: A method as in claim 6, wherein the authentication is valid only if the decrypted PIN and the PIN stored in the database are identical; if this is the case, the authentication server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.

Claim 8: An apparatus as in claim 1, wherein the smart card is powered by the voltage provided by the telephone line.

Claim 9: An apparatus as in claim 8, wherein the smart card transmits the modulated signal when the switch of the card reader is pressed by the user.

Claim 10: An apparatus as in claim 9, wherein the smart card transmits the modulated signal to the telephone line through the ISO contact C6.

Claim 11: An apparatus as in claim 10, wherein the smart card transmits the modulated signal when the ISO contact C2 is pulled down.

Claim 12: An apparatus as in claim 11, wherein the smart card is powered through the ISO contacts C4 and C8.

Claim 13: An apparatus as in claim 1, wherein the card reader is further integrated into the telephone handset.